This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/559,230	04/26/2000	Peter F. King	UWP1P026/1091	1263

26528 7590 10/04/2004

BWT-OPW
P.O. BOX 778
BERKELEY, CA 94704-0778

EXAMINER	
CURCIO, JAMES A F	
ART UNIT	**PAPER NUMBER**
2122	

DATE MAILED: 10/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/559,230	KING, PETER F.	
	Examiner	Art Unit	
	James Curcio	2122	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-40 of application 09/559230 remain pending.

Response to Arguments

1. Applicant's arguments filed August 13, 2004 have been fully considered but they are not persuasive.

With respect to argument (a), the broadest reasonable interpretation of "negotiating a privacy agreement" includes a handshake network protocol combined with a transfer of credential information, which is present in Winslett et al as pointed out in the previous office action and repeated below. Determining "what credentials are required by one party to service a particular request" as in the "extra round of communication" pointed out in the previous office action also constitutes a part of "negotiating a privacy agreement" because this communication requires the participation and negotiation of two parties, not just one.

With respect to argument (b), "matching credentials of one entity to the requirement of another entity does include an agreement (in similar words, correspondence or matching or consistency) between the two entities in the "broadest reasonable interpretation" of the word "agreement" (e.g. "agreement" means "accord" or "understanding" according to www.dictionary.com and act of being in accord according to The American Heritage College Dictionary Fourth Edition). Also, exchanging any information between two parties in any network setting involves an agreement or protocol for communication. So "determining whether a privacy agreement is needed" is indeed taught by Winslett et al as presented in the previous action.

With respect to argument (c), "establishing an authorization agreement" includes in its broadest reasonable interpretation, handshake protocol agreements that establish the communication of privacy credentials between two parties as taught in Winslett et al and addressed in the previous action.

With respect to argument (d), "accepting a proposed privacy agreement when in accord with the authorization agreement" includes in its broadest reasonable interpretation, one party's acceptance of a handshake proposal by another party in its request to communicate privacy credentials over a network to that one party as taught in Winslett et al and addressed in the previous office action.

With respect to argument (e), "negotiating a privacy agreement by a proxy server for a client device when the authorization agreement is not in accord with the authorization agreement" includes in its broadest reasonable interpretation handshake retries after failure to communication privacy credentials between two parties with a communication agreement as taught in Winslett et al and addressed in the previous office action.

With respect to argument (f), Applicant seems to suggest that the broadest reasonable interpretation of agreement is "formal document." The Examiner respectfully disagrees with this position because this interpretation of agreement is overly narrow to one of ordinary skill in the art. The broadest reasonable interpretation is more in line with two exemplary dictionary definitions presented earlier. (e.g. "agreement" means "accord" or "understanding" according to www.dictionary.com and

the act of being in accord according to The American Heritage College Dictionary Fourth Edition.)

Under this alternative definition of "agreement," Winslett et al clearly discloses or suggests "accepting the proposed privacy agreement when in accord with the authorization agreement, or negotiating the privacy agreement when not in accord with the authorization agreement."

The invalidity of (g) and (h) similarly arises from the overly narrow interpretation of "agreement" upon which the Applicant relies.

For at least these reasons, claims 1-36 remain rejected, arguments (a) – (h) notwithstanding.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 40 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 40 recites the limitation "said markup language" in line 1. There is insufficient antecedent basis for this limitation in the claim. Examiner interprets claim 40 as depending on claim 39.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-7, 9-23, and 34-37 rejected under 35 U.S.C. 102(b) as being anticipated by Winslett et al ("Assuring Security and Privacy").

6. As per claims 1 and 34, Winslett et al discloses the following:

a receiving step (see "set of credentials is submitted with a request for service" on page 143, 2nd column, 2nd paragraph),

a determining step (see "determines what credentials are needed for a particular service request" on page 142, 1st column, 1st paragraph),

a negotiating step (see "submitting them [the credentials] to the server" on page 142, 1st column, 2nd paragraph and see "this may require an extra round of communications with the server, which should be carried out automatically" on page 142, 2nd column 1st full paragraph), and

a producing step (see "sending the response to the client" on page 146, 2nd column, 1st partial paragraph).

7. As per claim 3, in addition to the teachings applied above, Winslett et al discloses steps for receiving the private information associated with the client device (see "SSA can use the credentials attached to the request" on page 145, 2nd column, 3rd full paragraph) and producing the response to the request based at least in part on the

private information (see "SSA . . . wishes to return an explanation to the PSA, the SSA can use the credentials attached to the request to determine what portion and version of its knowledge base it is willing to share" on page 145, 2nd column, 3rd full paragraph; and see "sending the response to the client" on page 146, 2nd column, 1st partial paragraph).

8. As per claim 6, in addition to the teachings applied above, Winslett et al discloses that the method is performed on a server (see "submitting them [the credentials] to the server" on page 142, 1st column, 2nd paragraph and see "this may require an extra round of communications with the server, which should be carried out automatically" on page 142, 2nd column 1st full paragraph).

9. As per claim 7, in addition to the teachings applied above, Winslett et al discloses that the private information is attached to the request (see "attaches them [credentials] to service requests" on page 142, 1st column, 1st paragraph).

10. As per claims 9 and 35, in addition to the teachings applied above, the preferred embodiment of Winslett et al discloses steps for the following:

establishing an authorization agreement that enables the proxy server to negotiate privacy agreements (see "the personal security assistant is to manage a client's credentials in accordance with the stated policies of the client"),

receiving a request (see "set of credentials is submitted with a request for service" on page 143, 2nd column, 2nd paragraph), and

receiving a proposed privacy agreement from the server device (see "policy on credential submission" on page 142, 2nd column, last paragraph to page 143, 1st

column, 1st partial paragraph, and see "SSA must also be able to export portions of its credential acceptance policy to clients who ask for explanations of its server's security policy" on page 143, 2nd column, 1st partial paragraph). The Office interprets that the server's security policy includes an explanation of how the server agrees to maintain the accepted credentials' security.

Winslett et al also discloses a step for accepting the proposed privacy agreement (see "determines what credentials are needed for a particular service request" on page 142, 1st column, 1st paragraph, see "assistant should cache information about what credentials are required for its client's most frequently and most recently accessed servers" on page 142, 2nd column, 1st full paragraph, see "policy on credential submission" on page 142, 2nd column, last paragraph to page 143, 1st column, 1st partial paragraph, and see "credential acceptance policy" on page 143, 2nd column, 1st partial paragraph). The Office interprets Winslett et al's using the credential acceptance policy and determining a credential submission policy based upon it to constitute acceptance of that policy.

Winslett et al additionally discloses a step for providing the private information to the server device (see "set of credentials is submitted with a request for service" on page 143, 2nd column, 2nd paragraph).

11. As per claims 2, 4, 5, 11, and 12, in addition to the teachings applied above, Winslett et al discloses that the private information includes client-provided location information of a client device associated with a network (see "credential", "University of

Illinois", "Faculty/Staff ID Card", "to access on-line services of the university libraries", and "driver's license" on page 141, 1st column, 1st full paragraph and last paragraph).

12. As per claims 13 and 14, in addition to the teachings applied above, Winslett et al discloses that the request including the private information associated with the client device is received at the proxy server (see "the proxy must intercept requests and then attach any needed credentials to them" on page 146, 1st column, last paragraph to page 146, 2nd column, 1st partial paragraph) and that the response is produced by the server device (see "SSA must also be able to export portions of its credential acceptance policy to clients who ask for explanations of its server's security policy" on page 143, 2nd column, 1st partial paragraph and see "proxy must examine responses to requests, looking for security-related information" on page 146, 2nd column, 1st partial paragraph).

13. As per claims 10 and 15, in addition to the teachings applied above, Winslett et al discloses that said providing operates to provide the private information to the server device after said accepting of the proposed privacy agreement as the privacy agreement or after said negotiating of the privacy agreement (see "submitting them [the credentials] to the server" on page 142, 1st column, 2nd paragraph and see "the personal security assistant must also be able to understand what credentials are required for a particular service request; this may require an extra round of communications with the server, which should be carried out automatically" on page 142, 2nd column 1st full paragraph).

14. As per claim 16, in addition to the teachings applied above, Winslett et al discloses that said providing operates to refuse to provide the private information to the

server device (see "which [credentials] should never be given out without explicit run-time permission" and "if any" on page 143, 1st column, 1st and 2nd paragraphs).

15. As per claim 17, in addition to the teachings applied above, Winslett et al discloses a step for determining whether an existing privacy agreement already exists (see "the use of server 'cookies' to retain state across interactions with a client" and "avoid resending credentials with subsequent service requests" on page 146, 2nd column, 1st full paragraph) and a step for bypassing said receiving of the proposed privacy agreement and said accepting of the proposed privacy agreement (see "avoid resending credentials with subsequent service requests" on page 146, 2nd column, 1st full paragraph).

16. As per claim 18, in addition to the teachings applied above, Winslett et al discloses steps for the following:

identifying an existing agreement between the server device and the client device, the existing agreement having a predetermined coverage (see "credential acceptance policy" on page 145, 1st column, 1st full paragraph) and

determining whether the request is covered by the predetermined coverage of the identified existing agreement (see "determines the set of roles that the client can assume for this kind of request, given the credentials submitted" on page 145, 1st column, 1st full paragraph).

17. As per claims 19, 20, and 36, in addition to the teachings applied above, Winslett et al discloses a step for the following:

receiving a request (see "set of credentials is submitted with a request for service" on page 143, 2nd column, 2nd paragraph);

determining whether a privacy agreement is needed (see "determines what credentials are needed for a particular service request" on page 142, 1st column, 1st paragraph, and see "policy on credential submission" on page 142, last paragraph to page 143, 1st partial paragraph); and

negotiating a privacy agreement that governs the exchange of private information when said determining determines that a privacy agreement is needed (see "submitting them [the credentials] to the server" on page 142, 1st column, 2nd paragraph and see "this may require an extra round of communications with the server, which should be carried out automatically" on page 142, 2nd column 1st full paragraph).

Winslett et al also discloses a step for determining, based on said privacy agreement, whether the server device is authorized to receive the private information (see "policy on credential submission" on page 142, last paragraph to page 143, 1st partial paragraph). The service requests in Winslett et al are categorized such that the resulting categories correspond to a classification of credentials in two sets according to the free or restrictive manner in which the service requests in that category may distribute them. The Office interprets the categorization of service requests to factor in the servers that receive these requests.

Winslett et al additionally discloses a step for providing the private information to the server device (see "set of credentials is submitted with a request for service" on page 143, 2nd column, 2nd paragraph.)

As per claims 21, 22, and 23, in addition to the teachings applied above, Winslett et al discloses a response to the request at the server device (see "sending the response to the client" on page 145, 2nd column, 1st partial paragraph).

As per claim 37, in addition to the teachings applied above, Winslett et al discloses that said method further comprises generating said privacy agreement and not exchanging private information which is not governed by said privacy agreement (same grounds as in the rejection of claim 1).

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 8-18, 25-26, 31-33, 35, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Winslett et al ("Assuring Security and Privacy") as applied to claims 1-7, 9-23, and 34-36 above.

20. As per claims 9-18 and 35, in addition to the teachings applied above, the preferred embodiment of Winslett et al discloses steps for the following:

establishing an authorization agreement that enables the proxy server to negotiate privacy agreements (see "the personal security assistant is to manage a client's credentials in accordance with the stated policies of the client"),

receiving a request (see "set of credentials is submitted with a request for service" on page 143, 2nd column, 2nd paragraph), and

obtaining a proposed privacy agreement (see "policy on credential submission" on page 142, 2nd column, last paragraph to page 143, 1st column, 1st partial paragraph).

Winslett et al also discloses a step for accepting the proposed privacy agreement (see "determines what credentials are needed for a particular service request" on page 142, 1st column, 1st paragraph, and see "policy on credential submission" on page 142, 2nd column, last paragraph to page 143, 1st column, 1st partial paragraph). The Office interprets Winslett's using a policy on credential submission to imply acceptance of that policy.

Winslett et al additionally discloses a step for providing the private information to the server device (see "set of credentials is submitted with a request for service" on page 143, 2nd column, 2nd paragraph).

Winslett et al's preferred embodiment fails to explicitly disclose that the privacy agreement is received from the server device associated with the request. However, an alternative embodiment of Winslett et al discloses this feature (see "a client has a list of qualifications that servers must meet before the client will do business with them" on page 149, 2nd column, 2nd full paragraph). The Office interprets these qualifications to include a server's agreement to a limited license to use the credentials provided by the client, the direct counterpart to a client's agreement to a limited license to use the services provided by the server in the preferred embodiment. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Winslett et al's preferred embodiment by including an agreement by the server to a limited license to use the credentials provided by the client in the manner taught by an

alternative embodiment of Winslett et al. One of ordinary skill in the art would have been motivated to do so in order for the client "to be careful in selecting the servers with whom it conducts business" (see page 149, 2nd column, 2nd full paragraph).

21. As per claims 8, 25, 26, 31, 32, and 33, in addition to the teachings applied above, Winslett et al discloses the following:

a proxy server device (see "personal proxy" on page 145, 1st column, last paragraph) and

a storage area (see "SSA must be able to reason about sets of credentials" on page 143, 1st column, last paragraph, and see "SSA firsts decrypts, parses, and verifies each credential" on page 143, 2nd column, 1st full paragraph). The Office interprets "decrypts, parses, and verifies each credential" to imply that the server security assistance includes a storage area that stores the credentials.

Winslett et al also discloses a privacy manager (see "credential acceptance policy" and "SSA must also be able to export portions of its credential acceptance policy to clients who ask for explanations of its server's security policy" on page 143, 2nd column, 1st partial paragraph; see "assistant should cache information about what credentials are required for its client's most frequently and most recently accessed servers" on page 142, 2nd column, 1st full paragraph; see "determines what credentials are needed for a particular service request" on page 142, 1st column, 1st paragraph; and see "policy on credential submission" on page 142, 2nd column, last paragraph to page 143, 1st column, 1st partial paragraph).

Official notice is taken that wireless client devices (e.g. battery-powered laptop computer) and wireless networks (e.g. Meier - US 5748619) have been well known and practiced in the computer art at the time the invention was made. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Winslett et al by including a wireless client device supported by a wireless network as the client and the network. One of ordinary skill in the art would have been motivated to do so in order to increase the portability of the client computers in a network setting and to increase access to the network.

22. As per claim 33, in addition to the teachings applied above, Winslett et al discloses that the information includes private information and non-private information and that the privacy manager restricts access to the private information but not the non-private information (see "the policy tells which credentials can be freely distributed and which should never be given out without explicit run-time permission" on page 143, 1st column, 1st partial paragraph).

23. Claim 24 rejected under 35 U.S.C. 103(a) as being unpatentable over Winslett et al ("Assuring Security and Privacy") as applied to claims 1-23, 25-26, and 31-36 above, and further in view of Baker et al (US005696898A). Winslett et al discloses a step for determining that the server device is authorized to receive the private information associated with the client device (see "policy on credential submission" on page 142, last paragraph to page 143, 1st partial paragraph). Winslett et al fails to expressly disclose that the determining step comprises comparing the URL of the request with a list of authorized URLs and determining that the server device is authorized to receive

the private information when the URL of the request is found within the list of authorized URLs. However, Baker et al discloses these features (see "various URLs that each user terminal should be allowed to transmit to public network 100" in Baker et al - column 4, lines 27-46). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Winslett et al by including steps for comparing the URL of the request and determining that the server device is authorized to receive the private information when the URL of the request is in the list of authorized URLs. One of ordinary skill in the art would have been motivated to do so in order to selectively control access to information (Baker et al - abstract).

24. Claims 27-30 and 39-40 rejected under 35 U.S.C. 103(a) as being unpatentable over Winslett et al ("Assuring Security and Privacy") as applied to claims 1-23, 25-26, and 31-36 above, and further in view of Gildea (US005523761A).

25. As per claims 27, 28, and 30, in addition to the teachings applied above, Winslett et al discloses that the information received from the client device and network comprises location information associated with the location of the client device as discussed above with respect to claims 2, 25, and 26. Winslett et al fails to expressly disclose a location manager that performs a reconciliation process on the location information received from the client device. However, Gildea discloses these features (see "correction of a computed location . . . based upon the corrections required to reconcile the GPS-determined location of the reference station with the known location of the reference station" in Gildea – column 22, claim 61, lines 20-29). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was

made to modify Winslett et al by including a location manager as per the teachings of Gildea. One of ordinary skill in the art would have been motivated to do so in order to determine the location of a reference station or client (Gildea – column 22, claim 61, lines 20-29).

26. As per claims 29, 39, and 40, in addition to the teachings applied above, Winslett et al fails to expressly disclose that the privacy agreement is provided in a markup language. Official notice is taken that it has been well known and practiced in the computer art to express information such as privacy agreements in markup languages such as HTML, XML, WML, and HDML to make this information reusable or computer platform-independent. Thus, accordingly such a claim would have been obvious.

27. As per claim 38, in addition to the teachings applied above, Winslett et al fails to expressly disclose that the said privacy agreement is negotiated in accordance with a Platform for Privacy Preferences (P3P) protocol. Official notice is taken that P3P protocols are well known in the computer art. Thus, accordingly such a claim would have been obvious to one of ordinary skill in the art at the time the invention was made.

Conclusion

28. Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Curcio whose telephone number is 703-305-8887. The examiner can normally be reached on Tuesday through Friday from 7 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tuan Dam, can be reached on Tuesday through Friday from 7:30 am to 4:30 pm and on alternate Mondays from 7:30 am to 4:30 pm. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

9/24/04
JC
AU 2122

TUAN DAM
SUPERVISORY PATENT EXAMINER